UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO

ALISON LAUSCHE, *individually and on behalf of all others similarly situated,* Plaintiff, v. BON SECOURS MERCY HEALTH, INC., Defendant.	Case No.: 1:24-cv-00594 **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Alison Lausche ("Plaintiff"), individually and on behalf of all others similarly situated, and on behalf of the general public, brings this Class Action Complaint, against defendant Bon Secours Mercy Health, Inc. ("BSMH" or "Defendant") based on personal knowledge and the investigation of counsel, and alleges as follows:

I. INTRODUCTION

1. With this action, Plaintiff seeks to hold Defendant responsible for the harms it caused Plaintiff and similarly situated persons in the preventable data breach of Defendant's inadequately protected computer network.

2. BSMH is one of the nation's 20 largest health care systems. With 48 hospitals, thousands of providers, over 1,000 points of care and over 60,000 employees Bon Secours Mercy Health serves communities across seven states.

3. As part of its business, Defendant obtained and stored the personal information of Plaintiff and Class members.

4. By taking possession and control of Plaintiff's and Class members' personal information, Defendant assumed a duty to securely store and protect it.

5. Defendant breached this duty and betrayed the trust of Plaintiff and Class members by failing to properly safeguard and protect their personal information, thus enabling cybercriminals to access, acquire, appropriate, compromise, disclose, encumber, exfiltrate, release, steal, misuse, and/or view it.

6. Defendant recently detected suspicious activity on its Workday test environment, indicating a data breach. Based on a subsequent forensic investigation, BSMH determined that cybercriminals infiltrated its inadequately secured Workday test environment and thereby gained undetected access to certain BSMH's data files between April 10, 2024 and July 31, 2024. The investigation further determined that, through this infiltration, cybercriminals potentially accessed and acquired the sensitive personal information of thousands of individuals.[1]

7. The personally identifiable information ("PII") accessed by cybercriminals included names, dates of birth, Social Security numbers, addresses, and other demographic information (collectively, "Personal Information").[2]

8. Defendant's misconduct – failing to implement adequate and reasonable measures to protect Plaintiff's and Class members' Personal Information, failing to timely detect the Data Breach, failing to take adequate steps to prevent and stop the Data Breach, failing to disclose the material facts that it did not have adequate security practices in place to safeguard the Personal Information, and failing to provide timely and adequate notice of the Data Breach – caused substantial harm and injuries to Plaintiff and Class members across the United States.

---

[1] *See Security Breach Notices: Bon Secours Mercy Health, Inc.*, South Carolina Department of Consumer Affairs (Oct. 10, 2024), https://consumer.sc.gov/sites/consumer/files/Documents/Security%20Breach%20Notices/BonSecoursHealthInc.pdf (last visited Oct. 18, 2024).

[2] *Id.*

9. Due to Defendant's negligence and failures, cyber criminals obtained and now possess everything they need to commit personal identity theft and wreak havoc on the financial and personal lives of thousands of individuals, for decades to come.

10. Plaintiff brings this class action lawsuit to hold Defendant responsible for its grossly negligent—indeed, reckless—failure to use statutorily required or reasonable industry cybersecurity measures to protect Class members' Personal Information.

11. As a result of the Data Breach, Plaintiff and Class members have already suffered damages. For example, now that their Personal Information has been released into the criminal cyber domains, Plaintiff and Class members are at imminent and impending risk of identity theft. This risk will continue for the rest of their lives, as Plaintiff and Class members are now forced to deal with the danger of identity thieves possessing and using their Personal Information.

12. Additionally, Plaintiff and Class members have already lost time and money responding to and mitigating the impact of the Data Breach, which efforts are continuous and ongoing.

13. Plaintiff brings this action individually and on behalf of the Class and seeks actual damages and restitution. Plaintiff also seeks declaratory and injunctive relief, including significant improvements to Defendant's data security systems and protocols, future annual audits, Defendant-funded long-term credit monitoring services, and other remedies as the Court sees necessary and proper.

II. THE PARTIES

14. Plaintiff is a citizen and resident of Hamilton County, Ohio.

15. Class Members are victims of the Data Breach and are domiciled both in and outside of Ohio. For example, thousands of Class members are citizens of South Carolina, as

evidenced by the South Carolina Department of Consumer Affairs' website, which shows that 8,696 residents of South Carolina were sent breach letters advising them that their information had been exposed in the Data Breach.[3]

16. Defendant is a Maryland corporation with its principal place of business in Cincinnati, Ohio.

III. JURISDICTION AND VENUE

17. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

18. The Class Action Fairness Act (CAFA) confers diversity jurisdiction to a class action where (1) the "matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs," and (2) "*any* member of a class of Plaintiff is a citizen of a State different from *any* defendant." 28 U.S.C. § 1332(d)(2) (emphasis added).

19. CAFA defines "class" as "all of the class members in a class action." 28 U.S.C. § 1332(d)(1)(A). CAFA further defines "class members" as "the persons (named or *unnamed*) who fall within the definition of the *proposed* or certified class in a class action." 28 U.S.C. § 1332(d)(1)(D) (emphasis added).

20. In this complaint, Plaintiff defines the proposed nationwide Class as: "All persons residing in the United States whose personal information was compromised during the Data Breach." *See infra*.

21. Class Members are victims of the Data Breach and are domiciled across the United States. For example, thousands of Class members are citizens of South Carolina, as evidenced by the South Carolina Attorney General's website, which shows that 8,696 residents of South Carolina were sent breach letters advising them that their information had been exposed

[3] https://consumer.sc.gov/identity-theft-unit/security-breach-notices (last visited Oct. 18, 2024).

in the Data Breach.[4] By having at least one "member of a class of Plaintiff [who] is a citizen of a State different from any defendant," diversity jurisdiction is conferred here, since the matter in controversy exceeds $5,000,000. *See* 28 U.S.C. § 1332(d)(2) (establishing that diversity jurisdiction is conferred where the amount in controversy exceeds $5,000,000 and where "*any* member of a [proposed] class of Plaintiff is a citizen of a State different from *any* defendant") (emphasis added).

22. This Court has personal jurisdiction over Defendant because Defendant conducts business in this District, maintains its principal place of business in this District, and has sufficient minimum contacts this State.

23. Venue is likewise proper as to Defendant in this District under 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). Venue is further proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

IV. FACTUAL ALLEGATIONS

A. The Data Breach and Defendant's Belated Notice

24. Defendant recently detected suspicious activity on its Workday test environment, indicating a data breach. Based on a subsequent forensic investigation, BSMH determined that cybercriminals infiltrated its inadequately secured Workday test environment and thereby gained undetected access to certain BSMH's data files between April 10, 2024 and July 31, 2024. The investigation further determined that, through this infiltration, cybercriminals potentially accessed and acquired the sensitive personal information of thousands of individuals.[5]

---

[4] *Id.*

[5] *See Security Breach Notice* letter, *supra*, https://consumer.sc.gov/sites/consumer/files/Documents/Security%20Breach%20Notices/BonSecoursHealthInc.pdf.

25. The Personal Information accessed by cybercriminals included names, dates of birth, Social Security numbers, addresses, and other demographic information.[6]

26. Despite the sensitivity of the PII that was exposed, and the attendant consequences to affected individuals as a result of the exposure, Defendant failed to disclose the Data Breach for several weeks from the time of the Breach. This inexplicable delay further exacerbated the harms to Plaintiff and Class members.

27. Based on the notice letter received by Plaintiff, the type of cyberattack involved, and public news reports, it is plausible and likely that Plaintiff's Personal Information was stolen in the Data Breach.

28. Upon information and belief, the unauthorized third-party cybercriminal gained access to the Personal Information, exfiltrated the Personal Information from Defendant's network, and has engaged in (and will continue to engage in) misuse of the Personal Information, including marketing and selling Plaintiff's and Class members' Personal Information on the dark web.

29. Accordingly, Defendant had obligations created by industry standards, common law, statutory law, and its own assurances and representations to keep Plaintiff and Class members' Personal Information confidential and to protect such Personal Information from unauthorized access.

30. Nevertheless, Defendant failed to spend sufficient resources on encrypting sensitive personal data, preventing external access, detecting outside infiltration, and training its employees to identify hacking threats and defend against them.

[6] *Id.*

31. The stolen Personal Information at issue has great value to the hackers, due to the large number of individuals affected and the fact the sensitive information that was part of the data that was compromised.

B. Plaintiff's Experience

32. Plaintiff received a notice letter from Defendant dated October 9, 2024, informing her that her Personal Information—including her Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

33. Plaintiff is very careful with her Personal Information.

34. Plaintiff would not have provided her Personal Information to Defendant had she known that Defendant would not utilize standard measures to reasonably secure her sensitive.

35. Because of the Data Breach, Plaintiff's Personal Information is now in the hands of cyber criminals. Plaintiff and all Class members are now imminently at risk of crippling future identity theft and fraud.

36. As a result of the Data Breach, Plaintiff has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including investigating the Data Breach, researching how best to ensure that she is protected from identity theft, reviewing account statements and other information, and taking other steps in an attempt to mitigate the harm caused by the Data Breach.

37. Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Personal Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Personal Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's Personal Information that was entrusted to Defendant with the understanding

that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's Personal Information; and (e) continued risk to Plaintiff's Personal Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information that was entrusted to Defendant.

C. Defendant had an Obligation to Protect Personal Information under the Law and the Applicable Standard of Care

38. Defendant also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

39. Defendant is further required by various states' laws and regulations to protect Plaintiff's and Class members' Personal Information.

40. Defendant owed a duty to Plaintiff and the Class to design, maintain, and test its computer and application systems to ensure that the Personal Information in its possession was adequately secured and protected.

41. Defendant owed a duty to Plaintiff and the Class to create and implement reasonable data security practices and procedures to protect the Personal Information in its

possession, including adequately training its employees (and others who accessed Personal Information within its computer systems) on how to adequately protect Personal Information.

42. Defendant owed a duty to Plaintiff and the Class to implement processes that would detect a breach on its systems in a timely manner.

43. Defendant owed a duty to Plaintiff and the Class to act upon data security warnings and alerts in a timely fashion.

44. Defendant owed a duty to Plaintiff and the Class to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Personal Information from theft because such an inadequacy would be a material fact in the decision to entrust Personal Information with Defendant.

45. Defendant owed a duty to Plaintiff and the Class to disclose in a timely and accurate manner when data breaches occurred.

46. Defendant owed a duty of care to Plaintiff and the Class because it was a foreseeable victim of a data breach.

D. Defendant was on Notice of Cyber Attack Threats and of the Inadequacy of their Data Security

47. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. Many members of the general public are familiar with the names of some of the biggest cybersecurity breaches: Target,[7] Yahoo,[8] Marriott

[7] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNet (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/ (last visited Oct. 18, 2024).

[8] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOOnline.com (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html (last visited Oct. 18, 2024).

International,[9] Chipotle, Chili's, Arby's,[10] and others.[11]

48. Defendant should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the Personal Information that it collected and maintained.

49. Defendant was also on notice of the importance of data encryption of Personal Information. Defendant knew it kept Personal Information in its systems and yet it appears Defendant did not encrypt these systems or the information contained within them.

E. Cyber Criminals Will Use Plaintiff's and Class Members' Personal Information to Defraud Them

50. Plaintiff and Class members' Personal Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and the Class members and to profit off their misfortune.

51. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[12] For example, with the Personal Information stolen in the Data Breach, identity thieves can open financial accounts, apply for credit, collect government benefits,

---

[9] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, The SSL Store: HashedOut (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/ (last visited Oct. 18, 2024).

[10] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNet (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b (last visited Oct. 18, 2024).

[11] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO Online (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (last visited Oct. 18, 2024).

[12] Insurance Info. Inst., *Facts + Statistics: Identity Theft and Cybercrime*, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Oct. 18, 2024) (discussing Javelin Strategy & Research's report *2018 Identity Fraud: Fraud Enters a New Era of Complexity*).

commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[13] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class members.

52. Personal Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[14]

53. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number and name.

54. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[15]

---

[13] John Egan, *What Should I Do if My Driver's License Number Is Stolen?*, Experian (June 13, 2024), https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last visited Oct. 18, 2024).

[14] U.S. Gov't Accountability Off., *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (July 5, 2007), https://www.gao.gov./products/gao-07-737 ("GAO Report") (last visited Oct. 18, 2024).

[15] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 18, 2024).

55. This was a financially motivated Data Breach, as apparent from the discovery of the cyber criminals seeking to profit off the sale of Plaintiff's and the Class members' Personal Information on the dark web. The Personal Information exposed in this Data Breach are valuable to identity thieves for use in the kinds of criminal activity described herein.

56. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[16]

57. Hackers may not use the accessed information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[17]

58. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[18]

59. With this Data Breach, identity thieves have already started to prey on the victims, and one can reasonably anticipate this will continue.

60. Victims of the Data Breach, like Plaintiff and other Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Data Breach.[19]

---

[16] Ari Lazarus, *How fast will identity thieves use stolen info?*, Fed. Trade Comm'n, U.S. Dept' of Defense, Consumer Financial Protection Bureau (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info (last visited Oct. 18, 2024).

[17] GAO Report, *supra*, https://www.gao.gov/products/gao-07-737.

[18] Fed. Trade Comm'n, *Guide for Assisting Identity Theft Victims*, 4 (Sept. 2013), archived at https://web.archive.org/web/20200621082937/http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (last visited Oct. 18, 2024).

[19] *Id.*

61. In fact, as a direct and proximate result of the Data Breach, Plaintiff and the Class have suffered, and have been placed at an imminent, immediate, and continuing increased risk of suffering, harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort and spend the money to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

62. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property including Personal Information;

b. Improper disclosure of their Personal Information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals and having been already misused;

d. The imminent and certainly impending risk of having their Personal Information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the data breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of individuals' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Personal Information; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

63. Moreover, Plaintiff and Class members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be incapable of protecting Plaintiff's and Class members' Personal Information.

64. Plaintiff and Class members are desperately trying to mitigate the damage that Defendant has caused them but, given the Personal Information Defendant made accessible to hackers, they are certain to incur additional damages. Because identity thieves have their Personal Information, Plaintiff and all Class members will need to have identity theft monitoring protection for the rest of their lives.

65. None of this should have happened. The Data Breach was preventable.

F. Defendant Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiff's and Class Members' Personal Information

66. Data breaches are preventable.[20] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[21] she added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[22]

67. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[23]

68. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

69. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any

---

[20]Lucy L. Thompson, *Despite the Alarming Trends, Data Breaches Are Preventable*, in *Data Breach and Encryption Handbook* (Lucy Thompson, ed., 2012).

[21]*Id.* at 17.

[22]*Id.* at 28.

[23]*Id.*

security problems.7 The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[24]

70. The FTC further recommends that companies not maintain Personal Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

71. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

72. Defendant failed to properly implement basic data security practices, including those set forth by the FTC.

73. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Personal Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

[24] Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business* (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 18, 2024).

74. Upon information and belief, Frontier failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiffs' and Class Members' Personal Information, resulting in the Data Breach.

75. Defendant was entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of Plaintiff's and Class Members' Personal Information.

76. Many failures laid the groundwork for the success ("success" from a cybercriminal's viewpoint) of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber security procedures and protocols necessary to protect Plaintiff's and Class members' Personal Information.

77. Defendant was at all times fully aware of its obligation to protect the Personal Information of Plaintiff and Class members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

78. Defendant maintained the Personal Information in a reckless manner. In particular, the Personal Information was maintained and/or exchanged, unencrypted, in Defendant's systems and were maintained in a condition vulnerable to cyberattacks.

79. Defendant knew, or reasonably should have known, of the importance of safeguarding Personal Information and of the foreseeable consequences that would occur if

Plaintiff's and Class members' Personal Information was stolen, including the significant costs that would be placed on Plaintiff and Class members as a result of a breach.

80. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class members' Personal Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiff's and Class members' Personal Information from those risks left that information in a dangerous condition.

81. Defendant disregarded the rights of Plaintiff and Class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its business email accounts were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class members' Personal Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class members prompt and accurate notice of the Data Breach.

V. CLASS ACTION ALLEGATIONS

82. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

83. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of the Class, defined as follows:

> All persons residing in the United States whose Personal Information was compromised as a result of the Data Breach.

84. Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

85. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

86. **Numerosity:** The proposed Class is believed to be so numerous that joinder of all members is impracticable. The proposed Subclass is also believed to be so numerous that joinder of all members would be impractical.

87. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive Personal Information compromised in the same way by the same conduct of Defendant.

88. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class that Plaintiff seeks to represent; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and Plaintiff's counsel.

89. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the

court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

90. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's Personal Information;

c. Whether Defendant's email and computer systems and data security practices used to protect Plaintiff's and Class members' Personal Information violated the FTC Act, and/or state laws and/or Defendant's other duties discussed herein;

d. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their Personal Information, and whether it breached this duty;

e. Whether Defendant knew or should have known that its computer and network security systems and business email accounts were vulnerable to a data breach;

f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

g. Whether Defendant breached contractual duties owed to Plaintiff and the Class to use reasonable care in protecting their Personal Information;

h. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

i. Whether Defendant continues to breach duties to Plaintiff and the Class;

j. Whether Plaintiff and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

k. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief;

l. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and members of the Class and the general public;

m. Whether Defendant's actions alleged herein constitute gross negligence; and

n. Whether Plaintiff and Class members are entitled to punitive damages.

VI. CAUSES OF ACTION

COUNT ONE

NEGLIGENCE

91. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

92. Defendant solicited, gathered, and stored the Personal Information of Plaintiff and the Class as part of the operation of its business and in order to gain revenues.

93. Upon accepting and storing the Personal Information of Plaintiff and Class members, Defendant undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so.

94. Defendant had full knowledge of the sensitivity of the Personal Information, the types of harm that Plaintiff and Class members could and would suffer if the Personal Information was wrongfully disclosed, and the importance of adequate security.

95. Plaintiff and Class members were the foreseeable victims of any inadequate safety and security practices on the part of Defendant. Plaintiff and the Class members had no ability to protect their Personal Information that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiff and the Class.

96. Defendant was well aware of the fact that cyber criminals routinely target large corporations through cyberattacks in an attempt to steal sensitive personal information.

97. Defendant owed Plaintiff and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

98. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures also have recognized the existence of a specific duty to reasonably safeguard personal information.

99. Defendant had duties to protect and safeguard the Personal Information of Plaintiff and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive Personal Information. Additional duties that Defendant owed Plaintiff and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, email accounts, protocols, policies, procedures and practices to ensure that Plaintiff's and Class members' Personal Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's and Class members' Personal Information in its possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its business email system, networks and servers; and

d. To promptly notify Plaintiff and Class members of any data breach, security incident, or intrusion that affected or may have affected their Personal Information.

100. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Personal Information that Plaintiff and the Class had entrusted to it.

101. Defendant breached its duty of care by failing to adequately protect Plaintiff's and Class members' Personal Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the Personal Information in its possession;

b. Failing to protect the Personal Information in its possession by using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees to avoid phishing emails;

d. Failing to use adequate email security systems, including industry standard SPAM filters, DMARC enforcement, and/or Sender Policy Framework enforcement to protect against phishing emails;

e. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Personal Information;

f. Failing to adequately train its employees to not store Personal Information longer than absolutely necessary for the specific purpose that it was sent or received;

g. Failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class's Personal Information;

h. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

i. Failing to promptly notify Plaintiff and Class members of the Data Breach that affected their Personal Information.

102. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

103. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

104. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Personal Information of Plaintiff and Class members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Personal Information of Plaintiff and Class members while it was within Defendant's possession and control.

105. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class members, Defendant prevented Plaintiff and Class members from taking meaningful, proactive steps toward securing their Personal Information and mitigating damages.

106. As a result of the Data Breach, Plaintiff and Class members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to fraudulent activity, closely monitoring bank account activity, and examining credit reports and statements sent from providers and their insurance companies.

107. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

108. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

109. In addition to its duties under common law, Defendant had additional duties imposed by statute and regulations, including the duties under the FTC Act. The harms which occurred as a result of Defendant's failure to observe these duties, including the loss of privacy, lost time and expense, and significant risk of identity theft are the types of harm that these statutes and regulations intended to prevent.

110. Defendant violated these statutes when it engaged in the actions and omissions alleged herein, and Plaintiff's and Class members' injuries were a direct and proximate result of Defendant's violations of these statutes. Plaintiff therefore is entitled to the evidentiary presumptions for negligence *per se*.

111. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant owed a duty to Plaintiff and the Class to provide fair and adequate computer systems and data security to safeguard the Personal Information of Plaintiff and the Class.

112. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Personal Information. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

113. Defendant gathered and stored the Personal Information of Plaintiff and the Class as part of its business, which affect commerce.

114. Defendant violated the FTC Act by failing to use reasonable measures to protect the Personal Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

115. Defendant breached its duties to Plaintiff and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to

safeguard Plaintiff's and Class members' Personal Information, and by failing to provide prompt and specific notice without reasonable delay.

116. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

117. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

118. Defendant breached its duties to Plaintiff and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Personal Information.

119. Defendant breached its duties to Plaintiff and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiff and the Class.

120. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

121. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence.

122. Plaintiff and the Class have suffered injury and are entitled to actual and punitive damages in amounts to be proven at trial.

COUNT TWO

BREACH OF IMPLIED CONTRACT

123. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

124. Plaintiff alleges this claim in the alternative to her breach of express contract claim.

125. Plaintiff and Class Members were required to provide Defendant with their Personal Information in order to receive financial services.

126. When Plaintiff and Class Members provided their Personal Information to Defendant when seeking these services, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties to protect their Personal Information and to timely notify them in the event of a Data Breach.

127. Based on Defendant's representations, legal obligations, and acceptance of Plaintiff's and the Class Members' Personal Information, Defendant had an implied duty to safeguard their Personal Information through the use of reasonable industry standards.

128. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' Personal Information, including through industry standard technologies like encryption, and failing to provide them with timely and accurate notice of the Data Breach. Indeed, it took Defendant *weeks* to warn Plaintiff and Class Member of their imminent risk of identity theft. Defendant also failed to notify Plaintiff and the Class Members whether or not their driver's license numbers were compromised, leaving Plaintiff and Class Members unsure as to the extent of the information that was compromised.

129. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff and the Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiff's and the Class Members' Personal Information.

COUNT THREE

UNJUST ENRICHEMNT

130. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

131. Plaintiff and the Class bring this claim in the alternative to all other claims and remedies at law.

132. Defendant collected, maintained, and stored the Personal Information of Plaintiff and Class members as part its business operations and to gain profits. As such, Defendant had direct knowledge of the monetary benefits conferred upon it.

133. Defendant, by way of its affirmative actions and omissions, including its knowing violations of its express or implied contracts with the entities that collected Plaintiff's and the Class members' Personal Information, knowingly and deliberately enriched itself by saving the costs it reasonably and contractually should have expended on reasonable data privacy and security measures to secure Plaintiff's and Class members' Personal Information.

134. Instead of providing a reasonable level of security, training, and protocols that would have prevented the Data Breach, as described above and as is common industry practice among companies entrusted with similar Personal Information, Defendant, upon information and belief, instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiff and Class members.

135. Defendant failed to implement—or adequately implement—data security practices, procedures, and programs to secure sensitive Personal Information, including without limitation those industry standard data security practices, procedures, and programs discussed herein.

136. As a direct and proximate result of Defendant's decision to profit rather than provide adequate data security, Plaintiff and Class members suffered and continue to suffer actual damages, including (i) the amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiff's Personal

Information, (ii) time and expenses mitigating harms, (iii) diminished value of Personal Information, (iv) loss of privacy, (v) harms as a result of identity theft; and (vi) an increased risk of future identity theft.

137. Defendant, upon information and belief, has therefore engaged in opportunistic and unethical conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiff and the Class in direct violation of Plaintiff's and Class members' interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

138. Accordingly, Plaintiff and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiff and the Class.

COUNT FOUR

BREACH OF FIDUCIARY DUTY

139. Plaintiff restates and realleges all preceding allegations as if fully set forth herein.

140. At all relevant times hereto, Defendant owed, and owes, a fiduciary duty to Plaintiff and Class Members, including its duty to keep Plaintiffs' and Class Members' Personal Information reasonably secure.

141. Defendant breached its fiduciary duty to Plaintiffs and Class Members by failing to implement sufficient safeguards and by disclosing Plaintiffs' and other Class Members' Personal Information to unauthorized third parties.

142. As a direct result of Defendant's breach of its fiduciary duty of confidentiality and the disclosure of Plaintiffs' and Class Members' confidential Personal Information, Plaintiffs and Class Members have suffered damages.

143. As a direct result of Defendant's breach of its fiduciary duty and the disclosure of Plaintiffs' and Class Members' Personal Information, Plaintiffs and Class Members have suffered and will continue to suffer damages, including, without limitation, (i) the untimely and/or inadequate notification of the Breach, (ii) improper disclosure of their Personal Information, (iii) loss of privacy, (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach, (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud (vi) the increased risk of identity theft, (vii) loss of the benefit of the bargain, (viii) loss of privacy, (ix) loss of confidentiality, and (x) embarrassment, emotional distress, and humiliation. At the very least, Plaintiffs and the Class are entitled to nominal damages.

COUNT FIVE

DECLARATORY JUDGMENT/INJUNCTIVE RELIEF

144. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

145. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

146. Defendant owes duties of care to Plaintiff and Class Members that require Defendant to adequately secure their Personal Information.

147. Defendant still possess Plaintiff's and Class Members' Personal Information.

148. Defendant do not specify in the notice of Data Breach letters what steps they have taken to prevent a data breach from occurring again.

149. Plaintiff and Class Members are at risk of harm due to the exposure of their Personal Information and Defendant's failure to address the security failings that lead to such exposure.

150. Plaintiff, therefore, seeks a declaration that (1) Defendant's existing security measures do not comply with its duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training their security personnel regarding any new or modified procedures;

d. Segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiff and Class Members for a period of ten years; and

h. Meaningfully educating Plaintiff and Class Members about the threats they face as a result of the loss of their Personal Information to third parties, as well as the steps they must take to protect themselves.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual damages, restitution, attorney fees, expenses, costs, and such other and further relief as is just and proper.

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:

i. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

iii. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

iv. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of

Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

v. Ordering that Defendant cease transmitting Personal Information via unencrypted email;

vi. Ordering that Defendant cease storing Personal Information in email accounts;

vii. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

viii. Ordering that Defendant conduct regular database scanning and securing checks;

ix. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

x. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats faced as a result of the loss of financial and personal information to third parties, as well as the steps they must take to protect against such occurrences;

d. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

DATED: October 18, 2024

/s/ Terence R. Coates

Terence R. Coates (0085579) – Trial Attorney
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

A. Brooke Murphy
(*pro hac vice* application forthcoming)
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
T: (405) 389-4989
E: abm@murphylegalfirm.com

Counsel for Plaintiff and the Proposed Class